11. Сравнения по модулю идеала. Вычеты. 12. Факторкольцо

Сравнение по модулю идеала

- Пусть K — коммутативное кольцо, I — идеал в K.

Коммутативное кольцо:

1) Ассоциативность +
2) Коммутативность +
3) Ноль
4) Обратный элемент по +
5) Дистрибутивность
6) Ассоциативность *
7) Коммутативность *

Идеал:

I подкольцо K (I ⊂ K, одни и те же операции + и *) и выполнено: $\forall x \in K$ и $\forall a \in I$: $ax \in I$, то есть при “перемножении” любого элемента из идеала на любой элемент из кольца, мы остаёмся в пределах идеала.

Определение 1.5. Пусть A — произвольное кольцо. Подмножество $I \subset A$ называется *идеалом*, если выполнено следующее:

I1: $\forall x, y \in I \; x + y \in I$;
I2: $\forall x \in I \; -x \in I$;
I3: $\forall x \in I$, $a \in A$ верно, что $ax \in I$.

Определение

Пусть $a, b \in K$. Тогда $a \equiv_I b$ (или, что то же самое, $a \equiv b \pmod I$), если и только если $a - b \in I$.

Лемма 10

$\equiv_I$ — отношение эквивалентности (то есть, рефлексивно, симметрично и транзитивно).

Доказательство. • $a \equiv_I a$, так как $a - a = 0 \in I$.

• Если $a \equiv_I b$, то $a - b \in I$. Значит, $b - a \in I$, откуда $b \equiv_I a$.

• Если $a \equiv_I b$ и $b \equiv_I c$, то $a - b, b - c \in I$. Значит, $a - c = (a - b) + (b - c) \in I$, откуда $a \equiv_I c$. □

(Рефлексивность: xRx выполнено для $\forall x \in X$

Симметричность: из xRy следует yRx

Транзитивность: из xRy и yRz следует xRz)

Комментарии к доказательству: 0 лежит в кольце по определению; в кольце по определению лежит обратный элемент; кольцо по определению замкнуто по сложению

Определение

Вычет по модулю идеала I — это класс эквивалентности по $\equiv_I$.

• Различные вычеты не пересекаются. Кольцо K разбито на вычеты.

То есть все элементы кольца разбиваются по кучкам (классам) и для каждой кучки (класса) находится такое I, что выполнено определение отношения эквивалентности для любых двух элементов из кучки.

Факторкольцо

• Для $a \in K$ вычет, состоящий из элементов кольца, сравнимых с a, как правило, будем обозначать через $\overline{a}$.

• Из определения следует, что $\overline{a} = a + I = \{a + x \ : \ x \in I\}$.

Определение

• Пусть K — коммутативное кольцо, I — идеал в K.
Факторкольцо $K/I := \{\overline{a} \ : \ a \in K\}$.

• $\overline{a} + \overline{b} := \overline{a+b}$; $\quad \overline{a} \cdot \overline{b} := \overline{ab}$.

Лемма 11

$+$ и $\cdot$ в K/I определены корректно.

Доказательство. • Пусть $a \equiv_I a'$, то есть, $\overline{a} = \overline{a'}$. Это означает, что $a - a' \in I$. Докажем, что от замены a на a' результат $+$ и $\cdot$ не изменится:

$$\overline{a}+\overline{b} = \overline{a'}+\overline{b} \iff a+b \equiv_I a'+b \iff a+b-(a'+b) = a-a' \in I;$$

$$\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b} \iff ab \equiv_I a'b \iff$$
$$ab - (a'b) = (a - a')b \in I \Leftarrow a - a' \in I. \qquad \square$$

Комментарии к доказательству: a и a’ сравнимы по модулю I и $\bar{a} = \overline{a'}$ это просто одна и та же запись. Потом добавили $\bar{b}$ к обеим частям равенства. Далее сказали, что $\bar{a} + \bar{b} = \overline{a + b}$, аналогично $\overline{a'} + \bar{b} = \overline{a' + b}$ (это факторкольцо)

Теорема 1

- *K/I с определенными выше $+$ и $\cdot$ — коммутативное кольцо.*
- *Если K — кольцо с 1, то K/I — тоже. Если при этом $a \in K$ — обратимый элемент в K, то $\bar{a}$ — обратимый в K/I.*

Доказательство. • Так как $\bar{a} + \bar{b} = \overline{a + b}$, из ассоциативности и коммутативности $+$ в K следует ассоциативность и коммутативность $+$ в K/I.

• Так как $\bar{a} \cdot \bar{b} = \overline{ab}$, из ассоциативности и коммутативности умножения в K следует ассоциативность и коммутативность умножения в K/I.

• Дистрибутивность:
$\bar{a}(\bar{b} + \bar{c}) = \overline{a(b + c)} = \overline{ab + ac} = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$.

• Ноль — это $\bar{0}$.

• Обратный по сложению: $-\bar{a} := \overline{-a}$.

• Единица: если $1 \in K$, то $\bar{1}$ — единица в K/I.

• Если $a \in K$ — обратимый, то $(\bar{a})^{-1} := \overline{a^{-1}}$ — обратный в K/I. □

Для коммутативного кольца:

1) Ассоциативность + (a+b)+c = a+(b+c)

$(a + b) + c \equiv_I a + (b + c)$ то есть $\overline{(a + b) + c} = \overline{a + (b + c)}$ то есть $\overline{(a + b)} + \bar{c} = \bar{a} + \overline{(b + c)}$, откуда $(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$

2) Коммутативность + a+b = b+a a+I+b+I = b+I+a+I

$a + b \equiv_I b + a$, то есть $\overline{a + b} = \overline{b + a}$, откуда$\bar{a} + \bar{b} = \bar{b} + \bar{a}$

3) Ноль
4) Обратный элемент по +
5) Дистрибутивность
6) Ассоциативность *

$(ab)c \equiv_I a(bc)$ то есть $\overline{(ab)c} = \overline{a(bc)}$ то есть $\overline{(ab)}\bar{c} = \bar{a}\overline{(bc)}$, откуда $(\bar{a}\bar{b})\bar{c} = \bar{a}(\bar{b}\bar{c})$

7) Коммутативность * ab = ba; $ab \equiv_I ba$, то есть $\overline{ab} = \overline{ba}$, откуда$\bar{a}\bar{b} = \bar{b}\bar{a}$